PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14

A1

(11) International Publication Number: WO 97/07463

(43) International Publication Date: 27 February 1997 (27.02.97)

(21) International Application Number: PCT/EP95/03186

(22) International Filing Date: 11 August 1995 (11.08.95)

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; Old Orchard Road, Armonk, NY 10504 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: PROBST, Jürgen [DE/DE]; Breite Strasse 44, D-72218 Wildberg (DE).

(74) Agent: RICHARDT, Markus; IBM Deutschland Informationssysteme GmbH, Patentwesen und Urheberrecht, D-70548 Stuttgart (DE).

(81) Designated States: JP, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

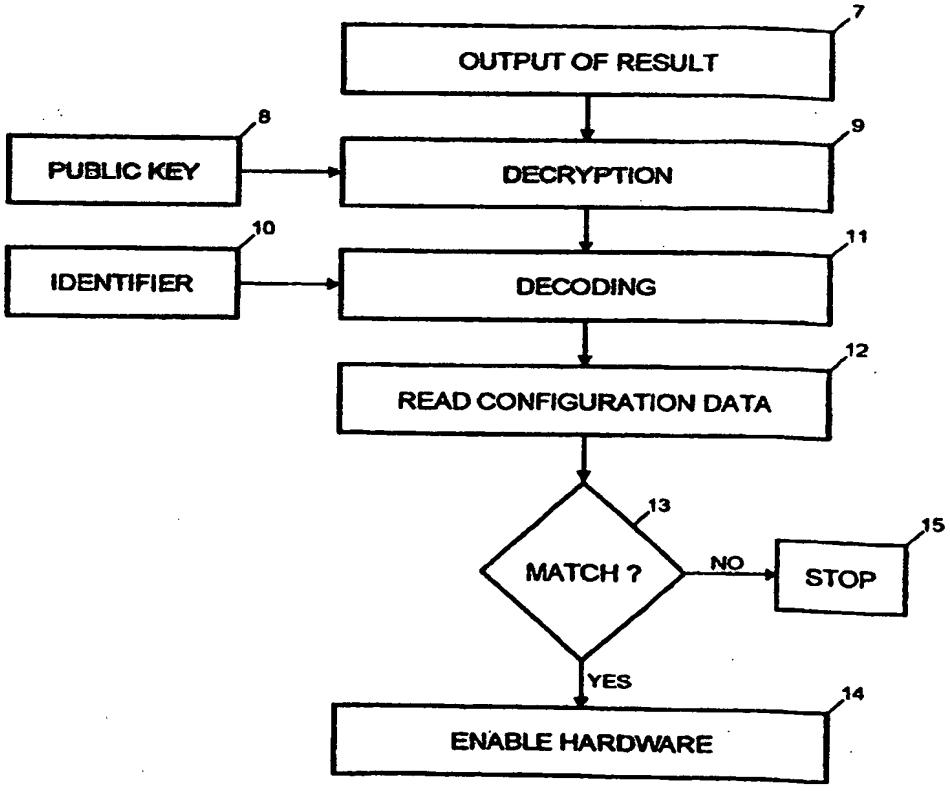
Published

With international search report.

(54) Title: METHOD FOR VERIFYING THE CONFIGURATION OF A COMPUTER SYSTEM

(57) Abstract

The invention relates to a method for verifying encrypted data being expressive of a configuration of a computer system, said computer system or a component thereof having an identifier, said method comprising the steps of encoding said data by an encoding method using said identifier as a key; encrypting said encoded data by an encryption method using a private key. For the decryption of the data a public key is used, preferably according to the RSA crypto system. The invention may also be used to enable functional characteristics of a computer system selectively.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

D E S C R I P T I O N

Method for verifying the configuration of a computer system

The invention relates to a method for verifying of a configuration of a computer system, to a method for encryption of data being expressive of a configuration of a computer system and to a computer system for carrying out such a method.

It is well known from the prior art to use passwords for security and verification purposes. There have been for many years password generators for a PIN. PINs have been used to gain access to automated tellers and security areas when unattended operation and/or verification of authorization is desired. They have been used for granting access to computers, as illustrated by U.S. Pat. No. 4,799,258 to Davies et al granted Jan 17, 1989. PINS may be generated automatically, and may be generated by random number generators or pseudo-random number sequences stored in the memory of a computer. US. Pat. No. 4,800,590 to James C. Vaughan illustrates a password generating device for generating passwords, and a computer access system based upon the generated secure number based on time such that the algorithm is valid only over a 3 minute window. However, the lock or unlock of a computer system e.g. the host computer of Vaughan does not satisfy needs which are now possible to achieve. It doesn't deal with repetitive modification of machine function and permits a range of numbers that can be matches instead of one unique number.

Many methods exist for granting or revoking a user's access to selected facilities or files within a data processing system. These techniques often utilize a

secret "key" or "password" entered by a user and recognized within the data processing system as an indication of the user's ability to read, write, delete, copy or append a selected record. One example of such a system is disclosed in U.S. Pat. No. 4,799,258. Further, several known techniques exist for storing such "keys," "passwords" or other secure data within secure storage devices within a data processing system. For example, U.S. Pat. No. 4,949,927 discloses a method for providing a security module for physically protecting such sensitive data. Similarly, U.S. Pat. No. 4,759,062 discloses a method for protecting sensitive data, such as private security codes.

Each of the methods described above permits the storage and utilization of sensitive or private data; however, none of these publications teaches a technique whereby the functional characteristics of a data processing system may be selectively altered. Systems do exist for enabling or disabling electronic equipment utilizing "keys" or other similar devices. Primarily such systems are directed to enabling or disabling reception of television or CATV signals within a television receiver. For example, see U.S. Pat. Nos. 4,577,224 and 4,471,379.

From US-A-5 200 999 a public key cryptosystem key management based on control vectors is known. This serves for encrypting the public and private keys of a cryptographic asymmetric key (public key) algorithm, when these keys are stored outside the secure boundary of the cryptographic facility (i. e., cryptographic hardware) and for decrypting these keys when they are processed or used within the secure boundary of the cryptographic facility. The encrypted keys may be kept in a cryptographic key data set belonging to the cryptographic system software or they may be managed by the

cryptographic application programs that use the keys. The public and private keys are encrypted by a system master key stored in clear form within the secure boundary of the cryptographic facility.

US-A-4 908 861 discloses a data authentication method using modification detection codes based on a public one way encryption function. According to this method a message of arbitrary length is transformed into a block of fixed length defined modification detection code (MDC). Although there are a large number of messages which result in the same MDC, because the MDC is a many-to-one function of the input, it is required that it is practically not feasible for an opponent to find them. In analyzing the methods, a distinction is made between two types of attacks, i.e., insiders (who have access to the system) and outsiders (who do not).

From TDB No. 11, April 1992, pages 376 - 383 the solution of a certain concurrence related to the RSA public key cryptosystem is addressed. The underlaying RSA public key cryptosystem is known from R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM 21, 2 (February 1978). In TDB Vol. 36, No. 10, October 1993, pages 413 - 416 a protocol is disclosed for one-way authentication in the asymmetric model. In this protocol, a prover convinces a verifier that the prover knows the factus of large composite number N. The prover does this in a way that it does not reveal the factors of N. This protocol is useful for the software licensing problem.

In electronic design, April 17, 1995, page 96, an overview of different encryption techniques, especially the RSA public key concept is given.

In US-A-5 365 587 a system is disclosed for selectively altering the functional characteristics of a data processing system without physical or mechanical manipulation by providing an access code from a remote personal identification number generator to a secure controller and store of the computer system. This enables remote authorization of change in function of the computer system, such as performance tune up, speeding clock time, changing function and like changes. The computer system is first manufactured having a predetermined set of functional characteristics. A multibit alterable code which includes a functional characteristic definition is then initially loaded into physically secure, nonvolatile memory within the data processing system, utilizing an existing bus, or a fusible link which may be opened after loading is complete. The functional characteristic definition is loaded from nonvolatile memory into a nonscannable register within a secure portion of a control logic circuit each time power is applied to the data processing system and the definition is then utilized to enable only selected functional characteristics. Alternate functional characteristics may thereafter be selectively enabled by entering a security code which matches one of a number of preloaded codes and an encoded alternate functional characteristic definition. The alternate functional characteristic definition may be enabled on a one-time, metered, or regularly scheduled basis and variable capability data processing systems may be implemented in this manner utilizing a single manufactured system, without the necessity of manufacturing and storing multiple data processing system models.

In summary, the prior art is silent as to the usage of encryption techniques to verify the configuration of a computer system.

The underlaying problem of the invention is to provide a method for verifying of a configuration of a computer system, a method for encryption of data being expressive of a configuration of a computer system and a computer system for carrying out such a method.

The problem of the invention is solved by the features laid down in the independent claims.

Data which is expressive of the configuration of a computer system advantageously is encrypted during manufacturing of the computer system. This is done by using an identifier which is assigned to the computer system or a component thereof during manufacturing. The private key which is used for the encryption of the encoded data is only known to the manufacturer of the computer system.

The RSA cryptosystem preferably is used for encryption of the encoded data (cf. R. L. Rivest, A. Shamir and L. Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, February 1978, Vol. 21, No. 2). For encoding the data by means of the identifier, the identifier can for example simply be added to the data. For decoding the identifier is subtracted later on from the encoded data. Also the DES method can be used whereby the identifier of the computer system is employed as a secret key (cf. Cheryl Ajluni, "Security Techniques Ensure Privacy", Electronic Design, April 17, 1995, page 98).

The encrypted data can be stored in any kind of storage device of the computer system, for example on an EPROM or on a diskette. The encrypted data can already be stored in the computer system during manufacturing. However, it is also possible to transmit the encrypted data to the

computer system via a telephone line, ISDN or other telecommunication means when the computer system is already installed at the customer. This is advantageous if the configuration of the computer system is changed. Than a new set of encrypted data reflecting the changed configuration of the computer system is transmitted and stored on the storage device of the computer system. This saves a service engineer of the manufacturer of the computer system from travelling to the customer side in order to change the encrypted data according to the new configuration.

Once the encrypted data is stored on a storage device of the computer system, the encrypted data is used for verifying the configuration. This serves to protect the computer system against unauthorized changes of its configuration. This can be a requirement for technical reasons or can serve as asset protection for the manufacturer of the computer system.

The first step for verifying the configuration is to receive the encrypted data. This is accomplished by reading the encrypted data from the storage device of the computer system on which the encrypted data has been stored during manufacturing or by receiving the encrypted data via a telecommunications link directly from the manufacturer. Than the encrypted data is decrypted, preferably using a public key of the RSA cryptosystem. This yields the decoded data which has been encoded by means of the identifier. The identifier is available in the computer system, preferably in electronically readable form. For example, the identifier can be stored in one of the components of the computer system by a number of fuses which are blown according to the identifier of that component. This identifier can also serve as an identifier for the entire computer system. In

order to prevent the clowning of the computer system with another computer system having another identifier, the identifier has to be unchangeable. This can be guaranteed by storing the identifier in a component of the computer system which is exclusively produced by the manufacturer of the computer system. It is also preferable that the identifier is unique. However, absolute uniqueness is normally not required. If for example every thousandth computer system which is manufactured by the same manufacturer has an identical identifier, this would be a sufficient degree of security.

If the private and the public key match and if the same identifier is used for the encoding and decoding of the data than this yields the data which is expressive of the configuration of the computer system stored during manufacturing. The configuration data of the computer system is also stored on a storage device of the computer system in unencoded form. These configuration data are compared to the decoded data. If there is a match between the decoded data and the unencoded configuration data this means that the customer is authorized to use this configuration of the computer system. Preferably, this method for verifying of the configuration is carried out by means of microcode every time the computer system is booted.

Alternatively - instead of decoding the decrypted data - it is also possible to encode the configuration data which is stored in an encoded form in the computer system and to compare the encoded data with the encoded configuration data.

If the data and the configuration data do not match it is possible not to enable or to disable the entire system. An alternative is to enable the computer system only

insofar as the data and the configuration data match. This can be advantageous in the following scenario: A customer is assumed to have purchased a memory expansion card for the computer system from a third party which is not authorized by the manufacturer of the computer system to deliver such memory expansion cards. The memory expansion card is inserted into the computer system and the configuration data which is normally stored on a hard disk of the computer system is changed correspondingly. This change of the configuration data can be carried out easily since the configuration data is present in the computer system in an unencoded and unprotected form. However, when the computer system is booted the encrypted data which is provided by the manufacturer of the computer system is decoded and decrypted and subsequently compared to the unencoded configuration data. In the example considered here the data and the configuration data match with the exception of the memory expansion card. As a consequence this memory expansion card is ignored and the computer system is initialized during the booting procedure so that the memory expansion card is not addressable. This can also be done with other functional characteristics of the computer system, such as the cycle time. A method for selectively altering the functional characteristics as such is known from US-A-5 365 587.

In order to circumvent the method for verifying of a configuration of a computer system a third party could analyze the microcode which serves to carry out this method and find a way to bypass the corresponding portions of the microcode. This can be prevented if the microcode is also protected against tampering. This can be accomplished for example by special check sums of the microcode which are predefined and checked by a special routine periodically. From IBM Technical Disclosure

Bulletin, No. 9, February 1992, pages 188 - 191 a mechanism for Trusted Computing Base definition and checking is known which could also be used to prevent a third party from altering or bypassing the microcode.

One way of carrying out the invention is described in detail below with reference to drawings which illustrate only one specific embodiment, in which:

Fig. 1 is a flow chart illustrating the method for encryption of data;

Fig. 2 is a flow chart illustrating the method for verifying of the configuration of the computer system;

Fig. 3 is a flow chart illustrating an alternative method for verifying of the configuration of the computer system; and

Fig. 4 is a schematic block diagram of a computer system which may be utilized to implement the method and system of the present invention.

In step 1 of the flow chart shown in Fig. 1 the configuration of the computer system is defined by the manufacturer of the computer system. This results in data which is expressive of the specific configuration of the computer system considered here. In step 2 a unique and unchangeable identifier of the computer system is defined. The identifier is stored in a portion of the computer system where it is protected against tampering. In this example the identifier is stored on the clock chip of the computer system which is a specialized card which can not be produced or delivered by any third party. The clock chip is personalized by blowing a number

of fuses according to the identifier. The identifier is used in step 3 to encode the data which is expressive of the configuration of the computer system. This is accomplished - in the prefered embodiment considered here - by simply adding the identifier which is assumed to be a string of binary data to the data which is expressive of the configuration. Any algorithm using the identifier as a key could be used for encoding of the data, if the identifier can also be used for decoding of the encoded data according to the algorithm.

In step 4 the private key required for the encryption algorithm is fetched. Subsequently, the encoded data is encrypted in step 5 by means of the private key. The resulting encrypted data of step 5 is stored in the computer system in step 6 for example in an EPROM of the computer system.

When the computer system is booted on the customer site this result of the encryption of step 5 is outputted by the EPROM (step 7). Then the public key which is required for decryption of result is fetched from the hard disk of the computer system. In step 9 the decryption of the result is carried out by means of the public key. In step 10 the identifier is read from the clock chip of the computer system. The result obtained by the decryption of step 9 is decoded by means of the identifier in step 11. In the example considered here this is accomplished by subtracting the identifier from the result obtained in step 9.

In step 12 the configuration data is read from the hard disk of the computer system. The configuration data is compared to the result of step 11 in step 13. If there is a perfect match the booting procedure normally continuous and all the hardware is enable as defined by the

configuration data in step 14. If there is no perfect match one possibility is to simply stop the booting procedure so that the entire computer system is not usable (step 15). Another possibility is to selectively enable the functional characteristics of the computer system insofar as there is a match between the result obtained in step 11 and the configuration data read in step 12.

Fig. 3 shows an alternative way of carrying out the method illustrated in Fig. 2. In step 16 of Fig. 3 the result obtained in step 6 is outputted from the EPROM of the computer system. The following steps 17 and 18 of Fig. 3 corresponds to the steps 8 and 9 of Fig. 2 and serve to decrypt the result which was outputted in step 16.

In step 19 the configuration data is read from the hard disk of the computer system. Step 19 in Fig. 3 corresponds to step 12 in Fig. 2. Subsequently the configuration data which is read in Fig. 19 is encoded in step 21 by means of the identifier which is fetched from the clock ship in step 20. The results of the decryption of step 18 and the encoding of step 21 are compared in step 22. Based on the comparison carried out in step 22 it is decided in step 23 whether the decrypted data of step 18 and the encoded data of step 21 match. If there is a match step 24 is carried out which corresponds to step 14 of Fig. 2. If there is no match step 25 is carried out which corresponds to step 15 of Fig. 2.

For an overview of the computer system, the data processing system which can be selectively altered for functional characteristics without physical or mechanical manipulation, refer to Fig. 4. Fig. 4. depicts a high level block diagram of a data processing system which may

be utilized to implement the method and system of the present invention. As illustrated, the data processing system includes a computer 26 having a data link 27 and an operator console 28 coupled in a manner well known in the art. Many of the high level components within computer 26 are depicted within Fig. 4 including main store 29, which serves as the main electronic storage within computer 26, and a central electronic complex 30 is also depicted. As will be explained in greater detail herein, central electronic complex 30 may include multiple multi chip modules which serve to perform the various functions of the central electronic complex, or alternately, central electronic complex 30 may be provided with a single high density circuit and including integrated circuit devices equivalent to several million transistors.

A service processor 31 is provided and is preferably coupled between operator console 28 and central electronic complex 30 to provide access to the functions and circuitry therein. A power supply 32 and input/output channels 33 are also typically provided in such a computer system, as those skilled in the art will appreciate.

Still referring to Fig. 4, the high level segments of central electronic complex 30 are illustrated. In a modern main frame computer such as the International Business Machines Corporation System/390 the central electronic complex typically includes 1 or more multiple chip modules which serve to address various functions within a central electronic complex. As illustrated within Fig. 4, central electronic complex 30 includes an SC module 34 which preferably serves to buffer and control the flow of data between main store 14, input/output module 35 and various processes within

computer 26. Input/output module 35 preferably serves to control and buffer data between input/out channels 33 and main store 29 in a manner well known in the art. Similarly, B-module 36 is provided to buffer and control instructions and data for the processor and CP-module 37 serves to execute instructions within computer 26. As those skilled in the art will appreciate, each of these multi chip modules 34, 35, 36 and 37 constitutes a highly complex electronic module which may include more than 100 integrated circuit devices, each equivalent to thousands or millions of transistors.

Additionally, as those skilled in the art will appreciate, a translation look aside buffer (TLB) is also provided and is utilized, in a manner well known in the art, to translate virtual memory address into real memory addresses within main store or other locations within computer 26.

Mainframe computers such as the International Business Machines Corporation System/390 may include multiple levels of functional capability which may be provided by altering the range of memory that may be accessed within a particular computer system, the number or percentage of processors which are enabled within a particular computer, the amount of usable cache memory within a particular computer and the processors speed and/or capability provided within a particular computer. Thus, by providing computer 26 with the capability of all these functional characteristics during the manufacturing process a selected subset or variations of those functional characteristics may be enabled utilizing the method and system of US-A-5 365 587.

Furthermore, the computer 26 comprises a clock chip 39 having the identifier stored therein by means of a number

of fuses. The identifier is unique, unchangeable and electronically readable by the service processor 31 to which the clock chip 39 is connected. The computer system shown in Fig. 4 further comprises a hard disk 38. The hard disk 38 serves to receive the encrypted data which is encrypted according to the method of the invention. The encrypted data can be stored on the disk 38 during manufacturing. If the configuration of the computer system is changed a new set of encrypted data can be stored on the disk 38 on the customer site. It is also possible to input the updated encrypted data via the channels 33 into the computer 26 and to store the updated encrypted data on the disk 38 under the control of the service processor 31. Every time the computer system depicted in Fig. 4 is booted the service processor 31 accesses the disk 38 in order to read the encrypted data. The service processor 31 also accesses the disk 38 to read the public key needed for decryption according to the RSA method. The decryption of the encrypted data read from the disk 38 is carried out by the service processor 31 whereby usage is made of the public key. When the service processor 31 accesses the clock chip 39 in order to read the identifier.

Subsequently, the service processor 31 decodes the decrypted data and compares the result with the actual configuration data stored in unencrypted form on the disk 38. Alternatively the service processor 31 is programmed to encode the actual unencrypted configuration data by means of the identifier in order to compare the decrypted data and the encoded actual configuration data.

In response to the comparison carried out in service processor 31 the computer system is enabled according to the actual configuration data if a perfect match occurs. The selective enabling of functional characteristics of

the computer system 26 advantageously is carried out according to the method disclosed in US-A-5 365 587. If the comparison carried out by the service processor 31 reveals that there is no perfect match this can cause the interruption of the booting procedure so that the entire computer system is disabled. Alternatively only those functional characteristics of the actual configuration data stored on disk 38 which match the encrypted data are enabled selectively.

It is also possible to program the service processor 31 to carry out the method of the invention not during the initialization of the computer system 26 but during normal operation. If a mismatch occurs this can lead to a shut down of the entire computer system 26.
Alternatively only those features of the computer system which correspond to configuration data which do not match the decrypted configuration data are disabled.

C L A I M S

1. A method for encryption of data being expressive of a configuration of a computer system, said computer system or a component thereof having an identifier, said method comprising the steps of

   a) encoding (3) of said data by an encoding method, said encoding method using said identifier as a key;

   b) encrypting (5) of said encoded data by an encryption method, said encryption method using a private key.

2. A method for verifying of a configuration of a computer system, said computer system or a component thereof having an identifier, said method comprising the steps of

   a) receiving (7) of encrypted data being encrypted according to the method of claim 1;

   b) decrypting (9) of said encrypted data using a public key;

   c) decoding (11) of said encoded data using said identifier as a key;

   d) comparing (15) said data with configuration data stored in said computer system.

3. A method for verifying of a configuration of a computer system, said computer system or a component thereof having an identifier, said method comprising the steps of

a) receiving (16) of encrypted data being encrypted according to the method of claim 1;

b) decrypting (18) of said encrypted data using a public key;

c) encoding (21) of configuration data stored in said computer system by an encoding method, said encoding method using said identifier as a key;

d) comparing (22) said encoded data with said encoded configuration data.

4. Method according to any one of the preceding claims wherein said encryption method is the RSA method.

5. Method for selectively enabling of functional characteristics of a computer system, said computer system or a component thereof having an identifier, said method comprising the steps of

a) verifying a configuration of said computer system by a method for verifying according to anyone of the claims 2, 3 or 4;

b) enabling of a functional characteristic of said computer system if said data and said configuration data match as regards said functional characteristic.

6. Method according to claim 5 said functional characteristic being a cycle time or an amount of memory addressable.

7. A computer system comprising means for carrying out a method according to anyone of the preceding claims.

8. A computer system comprising

means (38) for reception of encrypted data being encrypted according to the method of claim 1,

means (31) for decryption of said encrypted data, said means for decryption being adapted to use a public key,

means (31) for decoding said encoded data, said means for decoding comprising means for accessing said identifier, and

means (31) for comparing said data with configuration data stored in said computer system.

9. A computer system comprising

means (38) for reception of encrypted data being encrypted according to the method of claim 1,

means (31) for decryption of said encrypted data,said means for decryption being adapted to use a public key,

means (31) for encoding of configuration data stored in said computer system, said means for encoding being adapted to use said identifier as a key,

means (31) for comparing said encoded data with said encoded configuration data.

10. Computer system according to claim 7, 8 or 9 further comprising means for selectively enabling of a functional characteristic of said computer system.

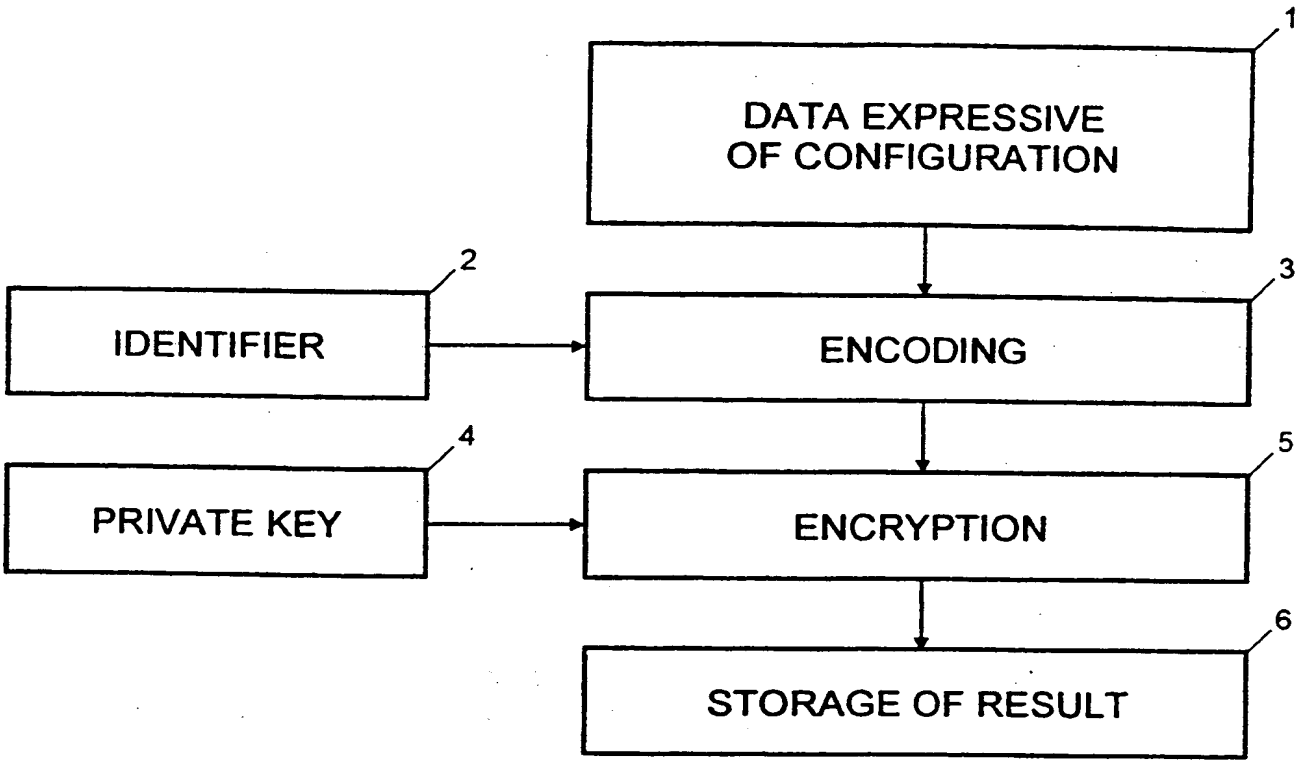

1
DATA EXPRESSIVE OF CONFIGURATION
2
IDENTIFIER
3
ENCODING
4
PRIVATE KEY
5
ENCRYPTION
6
STORAGE OF RESULT

Fig. 1

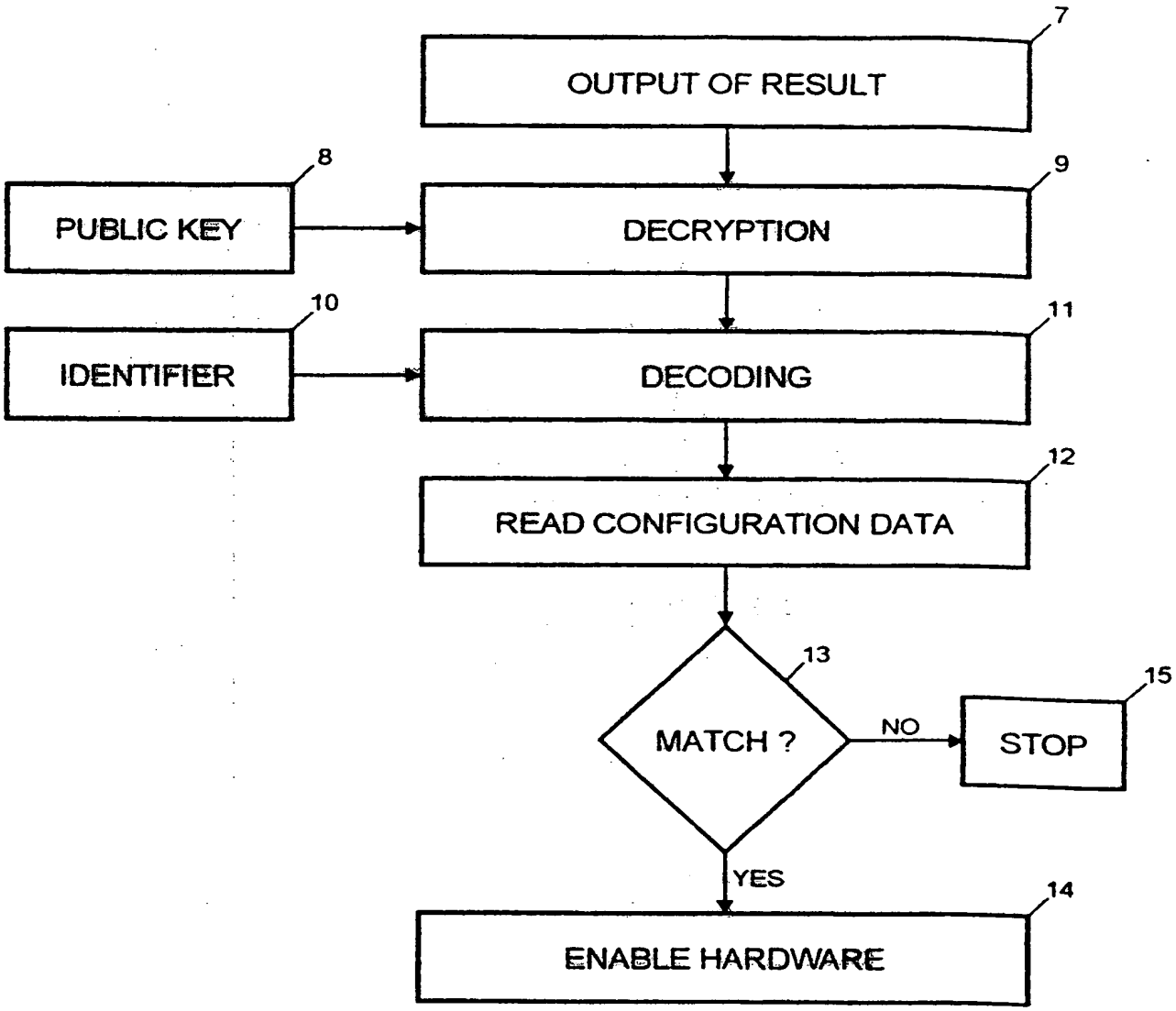

7
OUTPUT OF RESULT
8
PUBLIC KEY
9
DECRYPTION
10
IDENTIFIER
11
DECODING
12
READ CONFIGURATION DATA
13
MATCH ?
NO
15
STOP
YES
14
ENABLE HARDWARE

Fig. 2

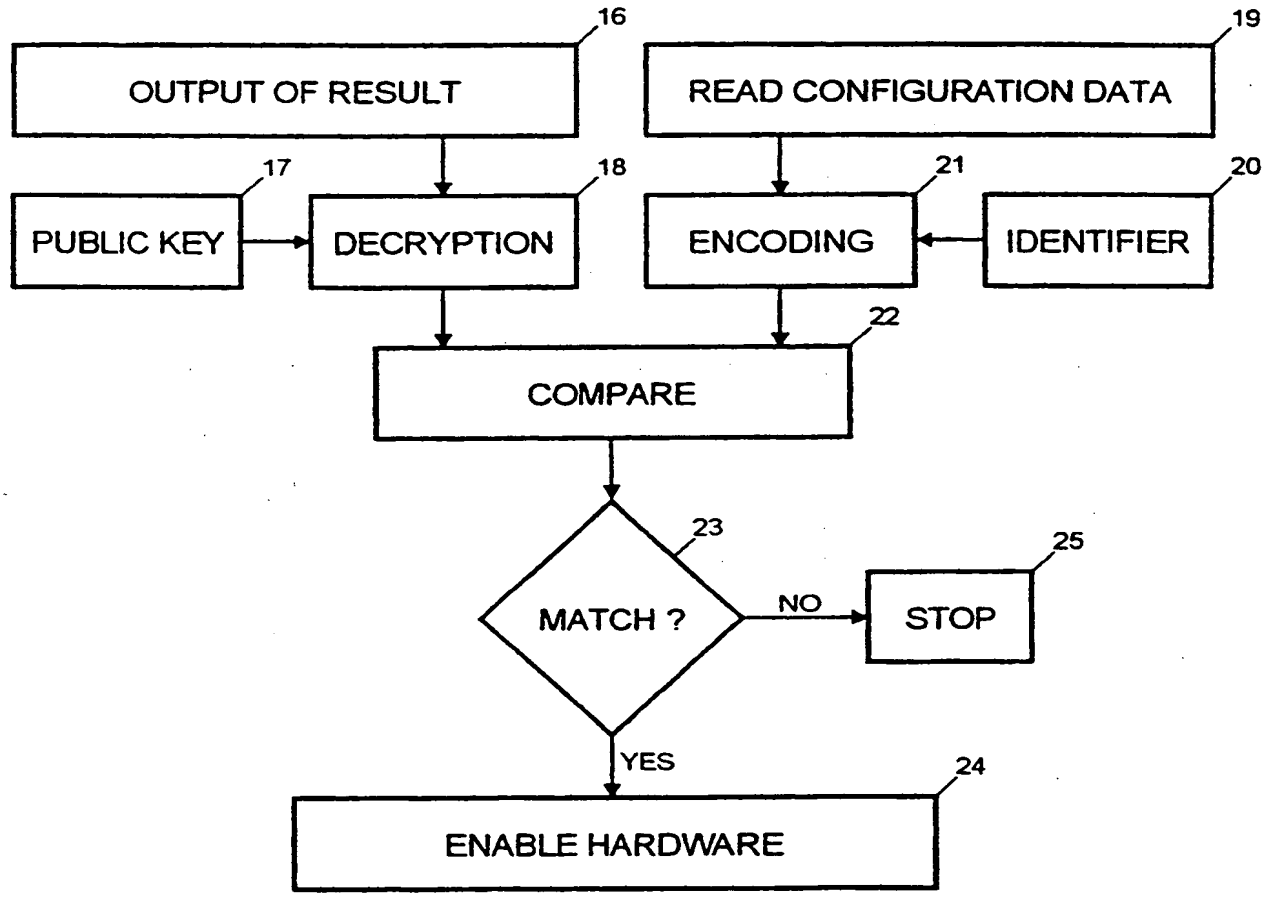

16
OUTPUT OF RESULT
19
READ CONFIGURATION DATA
17
PUBLIC KEY
18
DECRYPTION
21
ENCODING
20
IDENTIFIER
22
COMPARE
23
MATCH ?
NO
25
STOP
YES
24
ENABLE HARDWARE

Fig. 3

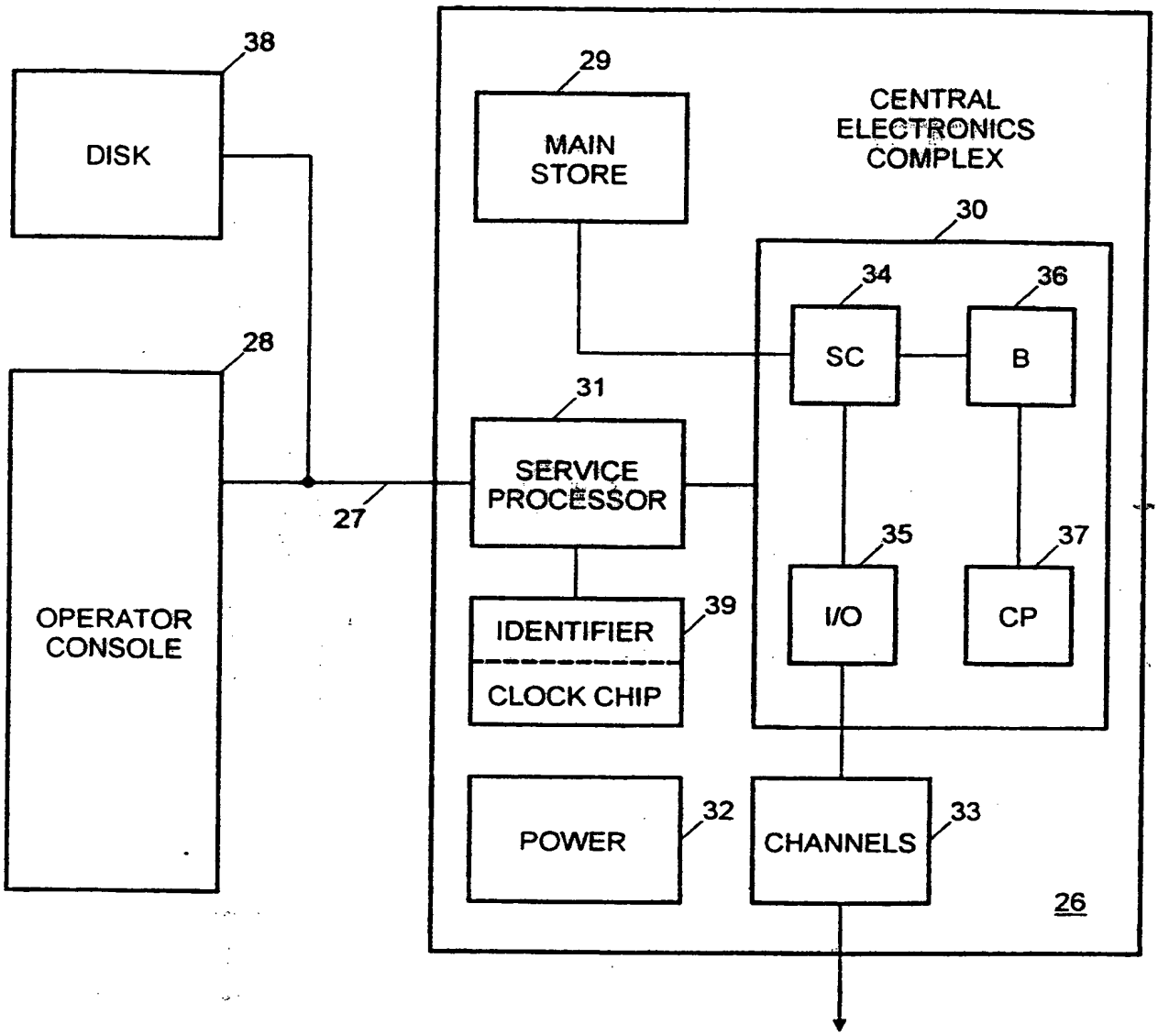

38
DISK
29
MAIN STORE
CENTRAL ELECTRONICS COMPLEX
30
34
36
SC
B
28
31
SERVICE PROCESSOR
27
OPERATOR CONSOLE
35
37
I/O
CP
IDENTIFIER
39
CLOCK CHIP
POWER
32
CHANNELS
33
26

Fig. 4

INTERNATIONAL SEARCH REPORT

ational Application No
PCT/EP 95/03186

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,5 182 770 (MEDVECZKY GEZA ET AL) 26 January 1993 see abstract; figures 2-4 see column 3, line 18 - line 34 see column 4, line 59 - column 5, line 12 see column 6, line 1 - column 8, line 34 see column 9, line 10 - line 28 see claims 1-17	1,2,4,5, 7-10
Y	---	3,6
Y	EP,A,0 388 839 (ALCATEL SATMAM) 26 September 1990 see abstract; figure 6 see claim 12	3
A	---	1,2,4-10
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 1996	22. 04. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Powell, D

Form PCT ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A,5 365 587 (CAMPBELL JOHN E ET AL) 15 November 1994 cited in the application see abstract ---	6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 95/03186

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5182770	26-01-93	NONE	
EP-A-0388839	26-09-90	US-A- 5077660	31-12-91
		DE-D- 69017485	13-04-95
		DE-T- 69017485	20-07-95
		US-A- 5369401	29-11-94
US-A-5365587	15-11-94	NONE	